IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Patentee	Yuh-Shen Song, et al.	**Examiner:**	James A. Kramer
Application No.:	10/647,158	**TC/Art Unit**	3627
Filing Date:	August 21, 2003	**Docket No.:**	7443-101/10310540
Title:	Anti-Fraud POS Transaction System	**Customer No.:**	000167
		Confirmation No.:	1808

APPLICANTS' BRIEF

1. REAL PARTY IN INTEREST

Yuh-Shen Song et al. (inventors of record).

2. RELATED APPEALS AND INTERFERENCES

None.

3. STATUS OF CLAIMS

Claims 1, 12, 16 and 17 were amended on 28 June 2005. Claims 2 through 11, 13, 14, 15 and 18 though 21 are pending as originally submitted. All claims were finally rejected on 20 September 2005. A Notice of Appeal was filed on 19 December 2005. Claims 1 through 21 are covered by this appeal.

4. STATUS OF AMENDMENTS

No amendments have been filed or entered subsequent to the final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As recited in **claim 1**, the invention provides a simple but elegant solution for minimizing fraudulent POS ("Point of Sale") transactions based on traditional payment instruments (i.e., checks, credit cards, etc.) which involves use of **using the same POS device (140 in both Fig. 1 and Fig. 3) to read (step 1001 & 1002, or 2001 & 2002) different information from two physically separate machine readable instrumentalities.** One of the instruments may be a conventional machine readable financial instrument (such as a check 120 in Fig, 1 or credit card 125 in Fig. 3) which provides information regarding **a financial institution and a specific account at that institution.** The other instrument may be a conventional machine readable government identification card (such as a driver's license 130 in both Fig. 1 and Fig. 3) which provides **payer's identification information**. The POS device then transmits (step 1003 or 2003) the locally read information from both instrumentalities, as well as the concerned transaction information **to a networked Validation and Processing Center** ("VPC") system (150 in both Figs. 1 and 3) which in turn is able to access **a remote database maintained by the financial institution (160 in Fig. 1 or 190 in Fig. 3)** containing account available balance information and account holder information for said specific account (step 1004 or 2004). See also paragraphs [0033] through [0036] & [0053] through [0056]. (All references to paragraph numbers are to the like numbered sections of published application US 2004/0138955 A1.)

The involved financial institution continues to have responsibility for maintaining the account information associated with the financial instrument while the government continues to be responsible for ensuring the integrity of the identification card. However, since both instruments can be automatically read by the POS terminal (paragraphs [0030] & [0033] and [0053]) and the information extracted from each sent electronically over a network to a remote "Validation and Processing Center" which is also networked to the financial institution's account database (paragraphs [0031], [0035]

and [0036] and [0050], [0055] and [0056]), it is now possible to automatically verify that the person withdrawing funds from the indicated account is properly authorized to make such a withdrawal by simply verifying that the embedded identification information read by the POS device from the government issued identification card matches (decision 1006 or 2006) the account holder information for the identified account stored in the remote database (paragraphs [0037] and [0038], and [0057] and [0058]).

Because it is government issued and presumably used for government purposes, the recited "machine-readable government issued identification card" and its "embedded identification information" will typically be protected not only by a number of security measures to prevent illegal copying or counterfeiting (paragraphs [0033], [0046]), but also by vigorous investigation of any suspected violations of the criminal law by the government personnel responsible for maintaining the integrity of the government issued identification cards. Moreover, as noted in paragraph [0051], in the unlikely event that such a card is lost or stolen, there is a high probability that the loss will be promptly noticed by the user and reported to the issuing authority.

Conversely, because the financial instrument merely has to identify a particular financial account at a particular financial institution and will only be accepted when presented in person by an authorized account holder whose identity has been verified by other means, the financial instrument need not contain any highly sensitive identification information, and indeed can be as simple as a traditional paper check imprinted with a magnetically encoded account number (paragraph [0034]).

In accordance with another aspect, as specifically claimed in claims 11 and 12, the VPC acts as an intermediary between the involved financial institutions and the payee (claim 11) and "secures the funds for the transaction against potential payer fraud" (claim 12). See also paragraphs [0036] through [0048] and [0058] through [0062].

In accordance with yet another aspect, as recited in claim 14 and described in detail in paragraphs [0039] and [0040], the financial instrument can be a conventional check imprinted with magnetically encoded account information, which may be marked "PAID" or otherwise rendered non-negotiable after the specified payment amount has been transferred.

Importantly, because sensitive data about the account holder can be stored remotely at the involved financial institution and because the sensitive transaction processing can be performed remotely at a secure VPC, many of the benefits of the present invention are available even with traditional negotiable instruments such as paper checks. In particular, even if the checks are stolen or counterfeit, it is highly improbable that the thief or counterfeiter will have physical possession of the account holder's government issued ID without being noticed and reported by the account holder to the government.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Representative claims 1, 12, and 14 (as well as related claims 2-11, 13, and 15-21) have been finally rejected as obvious under 35 USC §103(a) over Wheeler et. al., U.S. Patent No. 6,789,189 (hereinafter simply "Wheeler") either alone or in view of the Examiner's "Official Notice" that MICR lines on checks are conventionally used to communicate account information of the check user (which fact Applicants do not dispute).

Applicants contend that the Examiner's rejections are based on flawed construction of the claim language and/or on flawed reading of the cited Wheeler reference, in at least the following particulars:

Issues Common to the Rejections of All Three Representative Claims:

Whether Wheeler's teachings, which require the transmission of information that is highly confidential but susceptible to theft and thus require that this confidential

information be protected by using private-public key pair and digital signature technology, are even relevant to Applicants' invention?

Whether Wheeler actually teaches away from the use of a second machine readable instrumentality (i.e., government issued identification card) or whether Wheeler's ***optional*** Factors B and C are so broad as to include reading identity information from a second machine readable instrumentality (as apparently contended by the Examiner)?

Whether Wheeler is capable of achieving the same level of ***anti-fraud*** protection as Applicants' invention can achieve?

Issues Relevant Only to Representative Claim 12:

Whether Wheeler discloses or otherwise teaches that the networked validation and processing system which verifies the payer's authority to access the remote account is not only remote from the POS equipment and from the database containing the payer's account information, but also includes a separate financial institution which acts as an trusted intermediary between the payer's bank and the payee's bank?

Issues Relevant Only to Representative Claim 14:

Whether it would have been obvious to modify the system of Wheeler et al. to provide a means for conducting POS transactions by checks, and in particular, whether there is any motivation for using checks for POS transactions when Wheeler's device can already remotely conduct transactions for any financial account for which the user has access, including the user's checking account?

Whether Wheeler contemplates use of conventional financial instruments such as paper checks or whether Wheeler actually teaches away from the use of such conventional financial instruments?

Whether Wheeler discloses or otherwise teaches any mechanism for rendering a financial instrument (e.g., a conventional paper check) non-negotiable?

7. GROUPING OF CLAIMS

For proposes of this appeal, the present invention may be considered as including at least three separately patentable inventions:

I. Using information read from two physically separate machine readable instruments (i.e., a traditional financial instrument and a government issued identification card), which are processed by a networked validation and processing center having access to account holder information stored in a remote database of the financial institution, to verify the authority of the payer in conducting a POS transaction, as more specifically claimed in claim 1, which is hereby designated as representative of the group comprising of claims 1-10, 13, and 15-21 ("Group I").

II. The combination of claim 1 with the additional step of providing a third financial institution between the payer's financial institution and the payee's financial institution, as more specifically claimed in claim 11, which is hereby designated as representative of the group comprising claims 11 and 12 ("Group II").

III. The combination of claim 1 (wherein the financial instrument is a negotiable instrument, i.e., a check, with imprinted account information), with the additional step of rendering the check non-negotiable after the specified payment amount has been transferred, as specifically claimed in claim 14, which is hereby designated Group III.

Applicants hereby assert that the claims of each such Group should not stand or fall together with the claims of any other such Group.

8. ARGUMENT

a) Wheeler's and Applicants' Anti-Fraud Protection Technologies and Capabilities Are Fundamentally Different.

Wheeler contemplates a system 300 [Fig. 3] in which a single electronic device 350 may be used not only (1) to conduct secure communications 305, 309 between a user 302 and the ABDS database 310, but also (2) to retain a private key to retrieve the account identification information stored in the remote ABDS database for multiple accounts held at multiple institutions 312, and to (3) retain a mechanism for authenticating the card user 302 through Factor B or Factor C Entity Authentication methods. In effect, Wheeler's card 350 has become a new type of secure financial instrument that not only identities an account at a particular institution and other account related information, but also generates a digital signature which represents the authorization of the transactions by the holder of that instrument. Note that on column 15, lines 30-34, Wheeler actually teaches away from using a separate government issued ID card, since Wheeler's hardware token embodiment preferably takes the form of, inter alia, a card such as a credit card or ID badge. This fact is also evident from Wheeler's detailed description of the procedure of POS transactions (column 58, line 39 to column 61, line 20) that the only instrument required from a payer to conduct POS transaction is Wheeler's device.

Wheeler and Applicants use incompatible technological approaches. Wheeler requires consumers to replace all of their traditional payment instruments (such as checks, credit cards, debit cards, etc.) with a single sophisticated computational device which is secured using private-public key pair and digital signature technology, while Applicants' invention can be implemented with a relatively simple POS device which merely forwards (1) account identification information read electronically from traditional payment instruments; and (2) payer identity information read electronically from government-issued identification cards.

To identify the payer of a transaction, Wheeler must use the known public key information stored in the financial institution's database to first authenticate the ***device,*** which sends a digital signature through a private key stored inside the device. Wheeler's focus is on the security of the electronic communication ("EC") between the device and the database so that the device can be identified without any mistake, and hopefully, the payer can be ***indirectly*** identified once the device is ***directly*** identified. Therefore, the uniqueness of the private key in each Wheeler device is imperative to achieve this authentication goal. However, Wheeler has also pointed out that the chance for two of the Wheeler devices to have the same private key is not zero (column 16, line 24 to 28). Besides, the Wheeler devices can be easily stolen and used by third parties (e.g., thieves). The possibility of fraud is a real threat to the financial industry if only the Wheeler basic device is used. Thus, to avoid possible false identification of the payer, Wheeler ***requires*** the traditional Factor B Entity Authentication or Factor C Entity Authentication methods be used to positively identify that the payer is the actual owner of the device.

By contrast, Applicants' invention ***directly*** identifies the ***payer*** through government issued official identification cards. Since the physical possession of the government issued identification card is a prerequisite for use of Applicants' POS transaction system, the mere knowledge of payer's personal identification information is insufficient to complete a POS transaction. Consequently, the complicated private-public key pair and digital signature technologies, which are the core technologies used by Wheeler to identify the payer, are not even required. Since Applicants use the government issued identification card to authenticate the payer in a POS transaction, requiring the additional submission of Factor B or Factor C Entity Authentication information is not essential to authenticating the identity of the payer in Applicants' invention. ***In fact, even if consumers continue their resistance to Factor B Entity Authentication and Factor C Entity Authentication, Applicants' invention will still achieve its intended purpose.***

For anti-money laundering and anti-terrorist financing purposes, the USA PATRIOT Act and the Bank Secrecy Act require financial institutions to absolutely identify the ***"person"*** who conducts the transactions, not simply the ***"device"*** which is used for the transactions. Since Factor C Entity Authentication may intrude the privacy of consumers and may not be accepted by consumers, Factor B Entity Authentication, although inconvenient, may become the only possible means for authenticating the user of the Wheeler's device. Under such circumstances, a terrorist group or a money laundering group can use a person who has no prior criminal record to open multiple financial accounts and obtain multiple Wheeler devices, and each such device can be given to a different terrorist or a drug dealer to use. With Wheeler's device and the information required for Factor B Entity Authentication (such as a password, PIN number, etc.), each such terrorist or drug dealer can conduct financial transactions all over the world without being detected. ***In contrast, even if the government continues its enforcement of the Bank Secrecy Act and the USA PATRIOT Act and consumers continue their resistance to biometrical authentication (i.e., Factor C Entity Authentication), Applicants' invention still complies with the anti-money laundering and anti-terrorist financing regulatory requirements and laws, including the Bank Secrecy Act and the USA PATRIOT Act. Applicants' invention is not dependent on voluntary submission of private or confidential data.***

b) Wheeler Does Not Teach or Suggest the Use of a Separate "Machine-Readable Government Issued Identification Card" as Required by all Group I Claims.

Applicants and Wheeler are both concerned with providing means for authenticating the authority for conducting transactions initiated by a payer using a terminal device to access an account at a remote financial institution over a communication network, to effect a transfer of funds from the payer to a payee, and both use some sort of machine readable financial instrument to initiate such a transfer. In the case of Wheeler, the authority for conducting transactions is provided by his secure communication device

(350 in Fig. 3 or 6050 in Fig. 60) (which as noted in column, 15 lines 22-34, may take the form of a debit card, a credit card, or an ID badge, etc.). But the authentication means is fundamentally different: Wheeler uses the known public key information stored in the financial institution database to decode an electronic communication (EC) and thus authenticate the ***device,*** which may or may not be used by the true account holder, while Applicants use "account holder information" already known to the financial institution and stored in its database (such as driver's license information) and a government-issued official identification card (such as driver's license) to ***directly*** authenticate the ***payer*** as the account holder. Wheeler's focus is on the security of the electronic communication (EC) between the user's device and a remote secured database and contemplates that each user device will contain a private key that is securely embedded in the device such that it is protected from divulgation (column 11, lines 25-43). Wheeler assumes that any device having access to the private key ("Factor A") required for encoding the digital signature is authorized to access any account associated with the corresponding public key. Indeed, one of Wheeler's purported advantages is that these EC messages need not include any "identity" information in the message (column 12, lines 18-20). This is also evident in Wheeler's claim 16 (column 76, line 27 to 29). THUS WHEELER ACTUALLY TEACHES AWAY FROM APPLICANTS' CLAIMED INVENTION.

Wheeler does contemplate that additional authentication measures may sometimes be required to protect against physical theft of the user device, and to that end provides for Factor B Entity Authentication which is defined as a "Secret" that represents entity authentication based on "what the user or sender 'knows'" (such as PIN number, password, etc.) (column 17, lines 2-13)) and/or Factor C Entity Authentication which is defined as a biometric characteristic of the user (such as a fingerprint, DNA, etc.) that represents "what the sender 'is'" (column 17, lines 17-29). Preferably these Authentication Factors are used to personalize the device (column 16, lines 59-63), although Wheeler does observe that the authentication can take place remotely,

assuming that special precautions are taken to "prevent the interception and discovery by others" (column 17, lines 22-26)). In any event, neither Factor B nor Factor C is a separate machine readable government-issued identification card which provides identity information that must be matched with corresponding information stored at a remote financial institution, but rather is the actual private and confidential personal knowledge (i.e., Factor B) or biometric information (i.e., Factor C) which Wheeler requires to be provided by the user himself in order to activate the Wheeler device.

In contrast, Applicants are primarily concerned with authenticating not the payment instrument, but rather the ***true identity of the actual payer.*** Even more importantly, Applicants do not authenticate identity information, but rather they rely on governments to provide official identity information, whereby the user may be granted access to accounts previously associated with that user's identity information, and may be denied access to accounts that are not so associated. Moreover, since the identification information is maintained by the government on a government issued identification card, there is a high degree of confidence that the card and the embedded identification information will be protected from fraudulent alteration and misuse not only by government approved technical measures, but also by vigorous investigation of any suspected violations of the criminal law by the government personnel responsible for maintaining the integrity of the government issued identification cards.

Thus each of Wheeler's users must be provided with a unique special-purpose device which is in effect a totally new financial instrument, while Applicants' users are able to use conventional financial instruments (e.g., checks, etc.). Indeed, Applicants' users can also use these same conventional financial instruments in conventional terminals that use only conventional authentication technology.

In contrast, because Applicants contemplate the involved financial instrument merely has to identify a particular financial account at a particular financial institution, Applicants' recited financial instrument need not contain any highly sensitive information

and can even be in the form of a conventional paper check that is imprinted with MICR text that can be read by both humans and machines.

c) Wheeler Does Not Teach or Suggest the Provision of a Separate Financial Institution for Securing the Transaction Under the Control of the Verification and Processing Center ("VPC"), as Recited in Representative Claim 11.

As explained in column 11, line 46 and column 12, line 17, Wheeler's Intermediate Party 310 merely acts as a forwarding agent, forwarding the messages from the device 350 to the account authority 312 and then executing the instruction from the account authority 312 approving or rejecting the contemplated transaction by sending an appropriate notification to the account holder.

In contrast, as shown in detail, in steps 1013-1016 and 2013-2016 and as explicitly recited in claim 11 (which is dependent from claim 1), Applicants secure the transaction from fraud by either payee or payor by:

> transferring the specified payment amount from the payer's account to the VPC's bank system; and
>
> transferring the payment amount from the VPC's bank system to the payee's financial account.

Simply stated, Wheeler merely authenticates the equipment and secures the communications; Applicants' focus is on preventing fraud by the users (both payer and payee).

d) Wheeler is a Pure Electronic Solution That Has No Relevance to Conventional Paper-Based Instruments, As Recited in Representative Claim 14.

Claim 14 is dependent from claim 13, which recites:

> the transaction is based on a financial instrument in the form of a check drawn on the specified financial institution; and

the account and financial institution information is obtained by reading encoded information imprinted on the check;

Wheeler provides no means for reading such imprinted information from a paper check. On one hand, since Wheeler's device can already access a remote database to retrieve all the required account information of any financial account including a checking account, there is no motivation for including such a capability to read an imprinted check if the checking account already exists in the remote database maintained by the account authority. On the other hand, if a checking account does not exist in the remote database maintained by the account authority, even given a check, Wheeler's device cannot conduct any transaction for this checking account because the account authority simply has no authority over such an account at all. Therefore, checks do not exist in Wheeler's vision of the future; rather, Wheeler's device will replace all the traditional payment instruments, including checks.

e) Wheeler Does Not Teach or Suggest "Marking" the Financial Instrument (e.g., check) as "Non-Negotiable" After the Specified Payment Amount Has Been Transferred, As Recited in Representative Claim 14.

As a further fraud prevention measure which is especially relevant to conventional financial instruments such as paper checks, Applicants contemplate, as shown in steps 1013-1016 of Fig. 2, that the check will be marked "PAID" by the Merchant's POS terminal after the funds have been transferred to the VPC's bank, but prior to the transfer to the Merchant. The VPC's bank actually functions as an escrow agent in a POS transaction. There is simply nothing analogous in Wheeler's patent. Not only does Wheeler make no provision for processing paper-based financial instruments, Wheeler is not focused on preventing possible fraud by either the payer or the merchant through the traditional payment instruments.

9. CONCLUSION

In view of the arguments, the Examiner's rejections are unfounded and all claims are allowable over the prior art of record.

Respectfully submitted,

Dated: July 14, 2006

By: _____
John M. May
Reg. No. 26,200

Customer No. 000167
Fulbright & Jaworski L.L.P.
555 South Flower Street
Forty-First Floor
Los Angeles, CA 90071
Phone: (213) 892-9315
Fax: (213) 892-9494
E-mail: jmay@fulbright.com

10.9 APPENDIX

Copy of claims involved in the appeal

1. (Previously Presented) A method for verification and processing of a point of sale ("POS") financial transaction involving a payer's account at a financial institution, comprising:

identifying a financial institution and a specific account at that institution based on a machine readable financial instrument used in the transaction,

reading embedded identification information by the POS device from a machine-readable government issued identification card in the possession of the purported payer, wherein said machine readable financial instrument is physically separate from said machine readable identification card;

sending the payer's identification information, the identified financial institution and account information, and the transaction details read by the POS device to a Validation and Processing Center ("VPC") system through networks;

accessing by the VPC system through networks to a remote database maintained by the financial institution containing account available balance information and account holder information for said specific account;

verifying that the embedded identification information read by the POS device from the government issued identification card matches the account holder information for the identified account stored in the remote database;

verifying that the identified account has sufficient funds to cover a transaction amount specified by the payer; and

if the verification of both the identity of the payer and the amount of the transaction is successful, causing the specified amount to be electronically transferred from the specified payer's account to a designated payee.

2. (Original) The method of claim 1 further comprising:

prompting the payer to input into the POS device an additional item of personal information not embedded in the identification card but stored in the remote database of the financial institution, and

verifying that the additional personal information input by the payer matches the personal information stored in the remote database.

3. (Original) The method of claim 2, wherein the personal information input by the payer includes at least part of a social security number.

4. (Original) The method of claim 2, wherein the personal information input by the payer includes at least biometric information.

5. (Original) The method of claim 4, wherein the biometric information input by the payer includes at least a fingerprint.

6. (Original) The method of claim 1 further comprising:

prompting the payer to input into the POS device an additional item of personal information embedded in the identification card but not stored in the remote database of the financial institution, and

verifying that the additional personal information input by the payer matches the personal information embedded in the identification card.

7. (Original) The method of claim 6, wherein the additional personal information input by the payer includes at least a personal identification number.

8. (Original) The method of claim 6, wherein the additional personal information input by the payer includes at least biometric information.

9. (Original) The method of claim 8, wherein the biometric information input by the payer includes at least a fingerprint.

10. (Original) The method of claim 1 wherein the transaction details sent to the VPC system include the transaction amount, and the payee's financial account information.

11. (Original) The method of claim 1 wherein the completion of the funds transfer from the specified payer's account to a designated payee further comprises:
transferring the specified payment amount from the payer's account to the VPC's bank system; and
transferring the payment amount from the VPC's bank system to the payee's financial account.

12. (Previously Presented) The method of claim 1 wherein the VPC system secures the funds for the transaction against potential payer fraud.

13. (Original) The method of claim 1 wherein:
the transaction is based on a financial instrument in the form of a check drawn on the specified financial institution; and
the account and financial institution information is obtained by reading encoded information imprinted on the check.

14. (Original) The method of claim 13, wherein the financial instrument is marked as non-negotiable after the specified payment amount has been transferred from the specified payer's account.

15. (Original) The method of claim 13, wherein a magnetic ink character recognition device is incorporated into the POS device to read the account and financial institution information imprinted on the check.

16. (Previously Presented) The method of claim 1 wherein:
the transaction is based on a regular credit and/or debit card issued by a specified financial institution; and
the account and financial institution information is embedded in the card in a machine readable format.

17. (Previously Presented) The method of claim 16 wherein
a card reader is used to read the account and financial institution information contained in the credit and/or debit card, and
said information is embedded in the card in a machine readable format.

18. (Original) The method of claim 17, wherein a magnetic card reader is used to read the account and financial institution information contained in a magnetic strip of the card.

19. (Original) The method of claim 1, wherein:
the POS device is incorporated into a self-service checkout stand whereby customers may check out the goods and/or services by themselves.

20. (Original) The method of claim 1, wherein:
the VPC system is established exclusively for one financial institution to provide services to the customers of the financial institution.

21. (Original) The method of claim 1, wherein:
a wireless data transmission device is incorporated into the identification card; and

a wireless data receiver is incorporated into the POS device to read the machine-readable identification information of the identification card.